

Ministry of Foreign Affairs

UNCLASSIFIED / PUBLIC

Global Digital Compact Submission by the Kingdom of the Netherlands

Date 28 April 2023 Status FINAL

Colophon

Version Location Project manager(s) Contact Final The Hague, The Netherlands

Jacco-Pepijn Baljet Senior policy officer Cyber dvb-cyber@minbuza.nl Directorate for Security Policy

Enclosure(s)

Author(s)

Table of Contents

•	Colophon	3
•	Introduction	5
1	Connect all people to the Internet, including all schools	6
1.1	Core principles	6
1.2	Key commitments	6
2	Avoid internet fragmentation	7
2.1	Core principles	
2.2	Key commitments	
3	Protect data	8
3.1	Core principles	
3.2	Key commitments	
4	Apply human rights online	9
4.1	Core principles	
4.2	Key commitments	10
5	Accountability for discrimination and misleading content	10
5.1	Core principles	
5.2	Key commitments	11
6	Promote regulation of artificial intelligence (AI)	12
6.1	Core principles	12
6.2	Key commitments	12
7	Global Public Goods and Digital Commons	12
7.1	Core principles	13
7.2	Key commitments	13
8	Other topics – linked to trusted connectivity	13
8.1	Core principles	
8.1.1	Digital trust and security	
8.1.2	Sustainability	
8.2	Key commitments	
8.2.1	Digital trust and security	
8.2.2	Sustainability	

Introduction

.

The Kingdom of the Netherlands welcomes the open and transparent way in which the process of the Global Digital Compact has been designed and calls for continuing this inclusive approach in which all interested and relevant stakeholders are heard. In a similar spirit, we have included the Dutch internet community in the process of writing our national contribution. This submission is fully in line with the submission made by the European Union.

Due to the nature of the Internet, the incremental and valuable role of civil society, academia, the private sector as well as governments should always be considered. In that regard, the Netherlands strongly suggests to take into account the valuable outcomes of established processes, such as the conclusions of the Tunis Agenda and the WSIS+10 review which confirmed the multistakeholder model for Internet governance, the Messages of the Internet Governance Forum and Leadership Panel. Also the Global Digital Compact should underline the importance of an international multistakeholder platform, such as the annual Internet Governance Forum, to regularly debate Internet governance issues. The Global Digital Compact should explicitly build on and reinforce other commitments such as the UN Sustainable Development Goals. We must guard against duplication of ongoing UN processes, in particular topics which are currently being discussed in the First and Third Committee.

In outline, the Dutch contribution to the GDC focuses on:

- Bridging the digital 'divide', including promoting access and digital skills for women and girls, youth, groups or individuals in vulnerable situations, indigenous peoples, the elderly and persons with disabilities and special needs;
- Reaffirming and strengthening the multistakeholder model of internet governance;
- Strengthening linkages between human rights aspects and technical aspects of the standards development process;
- Mitigating the negative impact of (mass) surveillance, microtargeting, disinformation campaigns and internet shutdowns;
- Encouraging and emphasising the importance of 'Data free flow with trust', online privacy, online anonymity, confidentiality of electronic communications and strong encryption;
- Promoting international regulation of new and emerging technologies, with a human rights-based approach and assurance of the design, development, deployment, evaluation and use of technologies, platforms and tools.

1 Connect all people to the Internet, including all schools

1.1 Core principles

Increasing digitalization must not lead to exacerbated or reinforced inequality. To capitalize on the opportunities of the digital transition and to avoid or mitigate the risks involved, investments in digital infrastructure, universal access, digital inclusion, digital literacy and cyber security, including privacy, are of utmost importance. This digital transition must be underpinned by human rights safeguards to ensure the stability of societies and their economies. Increasing knowledge and skills to safeguard and protect the digital environment as a foundation for sustainable development is urgent and essential. Different levels of capacity among states might lead to a weaker resilience for all in our interconnected world.

Bridging the digital divide requires more than providing infrastructure and hardware. To foster digital inclusion and access to a safe digital environment we need to invest in the development of digital skills, such as digital literacy, the use of digital devices, communication applications, etc. This is in line with the UNSG's Roadmap for Digital Cooperation. Focus should also be given to digital education to ensure equity and inclusion. The education community, in particular teachers, should be adequately trained, skilled and equipped to incorporate technology effectively, ethically and responsibly in their teaching methods, and should also be enabled to teach digital technologies to ensure that students are better equipped to enter the labour market. Innovations in educational technology (EdTech) can give otherwise excluded children access to high-quality education.

Access to the Internet is also important for employment, especially youth employment. When people have access to the Internet, they are more capable of actively participating in the digital economy. And for this, additional skills are required. A report of the UN on the Human Development Index (2019) shows that for schoolchildren to participate in a digital society, advanced capabilities are needed. Such as problem solving skills, critical thinking skills and the ability to work in a team. Education and training are essential for broad personal development as well as to respond to the changing job market, to exploit the opportunities presented by digitalisation and to promote inclusiveness. Greater commitment to improving women's digital skills is crucial in pushing back on the widening gender gap on the international labour market.

1.2 Key commitments

Not being able to participate in the digital society magnifies inequality. Bridging this digital divide requires joint efforts from multiple parties, both on a national and an international level. Therefore, we are collaborating with public, private and civil society partners in order to make the Netherlands more digitally proficient and ensuring that everyone can (continue to) participate digitally, safely and healthily. At an international level, we collaborate on a diverse portfolio of projects. Via the EU's Global Gateway we support intercontinental initiatives focused on the accessibility and reliability of the digital environment, such as the installation of submarine cables between Europe, Africa and Latin America to increase the speed and accessibility of the internet. We reaffirm our commitment to working with the international community to close digital divides, including the gender digital divide.

The Global Digital Compact should call upon all Member States to connect all the unconnected, with a critical emphasis on women and girls, youth and vulnerable groups, indigenous peoples, the elderly, and persons with disabilities and specific needs.

The Netherlands strives to break down the gender digital divide entirely. While technological change and digitalization can accelerate progress for gender equality and the empowerment of all women and girls, but also under-represented or marginalized groups, it can also exacerbate vulnerabilities, existing inequalities, gender stereotypes and discriminatory social norms with serious risks and implications. The gender digital divide persists also in access to science, technology, engineering and math (STEM) education. This year's theme of International Women Day "DigitALL: Innovation and technology for gender equality" underlined the importance of this topic. The Global Digital Compact should include a commitment to achieving gender equality and empowering all women and girls by enhancing education and participation in cyberspace as users, content creators, employees, entrepreneurs, innovators and leaders.

2 Avoid internet fragmentation

2.1 Core principles

The multistakeholder model of Internet governance has been instrumental in maintaining an open, free, secure, interoperable, decentralized and resilient global Internet infrastructure. Restrictions of and on the Internet may threaten the global, open, free and secure nature of cyberspace, as well as the rule of law and human rights and fundamental freedoms, which apply offline as well as online. In order to preserve and improve the multistakeholder model, meaningful participation from all stakeholders on equal footing, should be guaranteed in Internet organisations and platforms as ICANN, IETF, IGF and further encouraged in ITU. An important positive effect of the multistakeholder model is that no stakeholder group has the sole responsibility to manage the internet or possibility to influence the functioning of the internet substantially. Especially participation from global majority countries and from under-represented or marginalized groups, should be encouraged.

The Global Digital Compact should address Internet fragmentation on two layers: the technical layer and the user experience or application layer. At the same time, the diversity and decentralization of the Internet infrastructure, in contrary to decoupling, should not be mistaken for fragmentation. These are core characteristics that underly the very nature of the Internet and support its resilience and its flexibility to adapt to changing circumstances.

2.2 Key commitments

The Global Digital Compact should reaffirm and strengthen the multistakeholdermodel of Internet governance. Participation on equal footing in the Internet organisations is instrumental in keeping the global internet open, free, secure, interoperable, decentralized and resilient.

The Global Digital Compact should commit to avoiding a fragmentation of the technical infrastructure of the Internet, impeding the ability of systems to

interoperate, and threatening the general integrity and availability of the core Internet infrastructure. This includes packet routing and forwarding, naming and numbering systems, encryption [technologies], and the underlying physical infrastructures.

A key feature of the open, free, secure and interoperable Internet is the free flow of information, which enables development, allows all to benefit optimally from access to the Internet and empowers individuals to exercise their universally applicable human rights, such as the freedom of expression. National and international policies and legislation that hamper, limit or block internet access, in ways not aligned with international human rights law, even if they are adopted with best intentions, should be avoided by taking a holistic approach to the protection and promotion of human rights and fundamental freedoms. Governmental Internet shutdowns have a disproportionately negative impact on human rights, economic welfare and innovation and could be avoided by taking alternative measures to address disinformation or other harmful content online in line with universally established principles such as necessity, proportionality, and legality. The Global Digital Compact should therefore commit to refrain from government-imposed Internet shutdowns.

3 Protect data

3.1 Core principles

The adequate protection of personal data is a key enabler of enhancing trust in the digital ecosystem. Users of digital technologies should be able to have full confidence that their personal data are processed and stored in a safe and secure way, not accumulated in an unlawful manner, and only accessed by those with the permission to do so. Maintaining the confidentiality, integrity and availability of personal and non-personal data is vital in this regard, including through the use of encryption. This way individuals have enhanced control over their (sensitive) personal data, and the trusted use of digital technologies is promoted.

Key principles for the protection of personal data online are the following: 1) Lawfulness, fairness, and transparency; 2) Purpose limitation; 3) Data minimization; 4) Accuracy; 5) Storage limitation; 6) Integrity and confidentiality; 7) Accountability.

These principles could be underpinned by an appropriate (national) legal framework, which adds to legal clarity and certainty for both users and businesses. While at the same time ensuring that cross border free flow of data should be possible to facilitate digital trade and development of a digital economy. For instance, countries could criminalize the interception and interference with computer data without a legal basis and when committed intentionally. Also, a commitment to the once-only principle, which states that citizens should not be forced to provide information to authorities if another authority already holds that information in electronic format, could be encouraged by fostering public administrations to re-use data, where possible and in accordance with the data protection rules, so that no additional burden falls on citizens or businesses. Governments, businesses and product designers themselves should also take into account these principles and work from a basis of privacy-by-design when developing new products and technologies.

3.2 Key commitments

Proportionate and secure sharing of data, including through cloud services, is and will be a vital component of a thriving digital economy. For this to materialize, it is important to have a strong data protection framework in place. The Compact could include a commitment to collaborate on the interoperability of such national frameworks, such as the "Data Free Flow with Trust"¹ framework with the additional mentioning of the importance of online privacy, online anonymity, confidentiality of electronic communication and strong encryption. Localization requirements, to process and store data locally, could actually lead to restrictions on data flows and inadvertently undermine privacy and security of data while hurting economic development. The negotiations in the WTO Joint Statement Initiative about ecommerce could offer an example of compromises of how to ensure cross border data flows while at the same time respecting countries' policy objectives, like protection of personal data and privacy.

4 Apply human rights online

4.1 Core principles

It must be recognized that international law, including international human rights law, applies equally offline as it does online. Human rights, such as the International Covenant on Civil and Political Rights (ICCPR), the International Convention on Economic and Social Rights (ICESR), the Convention on the Elimination of all forms of Discrimination Against Women (CEDAW) and the Convention on the Rights of the Child do therefore apply in the digital domain. Given the rapid technological developments and to create transparency and coherence around the application of the normative framework for responsible State behaviour, the question States should (continue to) address is how human rights law applies. The Compact can play an important role, for instance as a catalyst for these discussion, stimulating a united approach for these protection of human rights online.

Besides states, companies also have a responsibility to respect human rights online. The responsibility that companies have is laid down in, among others, the OECD Guidelines for Multinational Enterprises and the UN Guiding Principles on Business and Human Rights (UNGPBHR). However, existing commitments, such as the UNGPBHR, need updating to equally protect and promote human rights online and offline.

Emerging technologies can strengthen democratic institutions and democratic resilience, but at the same time they pose serious challenges to the promotion, protection and enjoyment of human rights, both online and offline. The Netherlands recognizes the importance of sustainable support to civil society organisations and women human rights defenders in particular who strive to protect and promote human rights and gender equality in the digital sphere. Women human rights defenders are more often at risk of threats and attacks, and their activities hampered by Internet restrictions and shutdowns.

¹ https://www3.weforum.org/docs/WEF_Data_Free_Flow_with_Trust_2022.pdf

Technical standards provide a common language that can enhance trust, security, and interoperability. Standardisation in the digital domain takes place in a broad spectrum of multilateral and multistakeholder organisations, including but not limited to ISO/IEC, IEEE, 3GPP, IETF, W3C, ITU, sector specific international organisations such as ICAO, IMO and lots of regional and private collaborations. The standards these bodies produce and the way those standards get implemented and adopted often provide ways to protect fundamental rights, but choices in the development of standards or during implementation can also inflict harm on human rights.

4.2 Key commitments

Human rights and fundamental freedoms should be reinforced throughout the GDC and a commitment to gender equality, non-discrimination and strong attention to marginalized groups should be integral to the Compact as a whole. The incremental role of the UN Office of the High Commissioner on Human Rights as leading entity in the UN on human rights should be acknowledged, as well as the relevance of existing commitments, such as the UNGPBHR and the Beijing Platform for Action.

As technical standards are at the core of the development and use of existing and emerging technologies, human rights and gender equality should be taken into account in the standard-setting process to ensure the application of human rights online and offline, including the development and implementation of standards. Standards should be consistent with international human rights law, respect fundamental freedoms and promote gender equality. The Netherlands calls for stronger linkages between the human rights and technical angle of standards development. We recognize the value of the continuation and intensification of the involvement of all stakeholders in the standardization process, including human rights experts. The Compact should acknowledge the fact that 'technical' standards development processes are not merely technical, but can have an impact on the promotion and protection of human rights.

The Compact should include a commitment to combat all forms of discrimination online, with a specific attention to multiple and intersecting forms of discrimination, including on grounds of sex, race, ethnic or social origin, religion or belief, political or any other opinion, disability, age, sexual orientation and gender identity. Also the negative consequences of (mass) surveillance, microtargeting, disinformation campaigns and online gender-based violence should be addressed.

Moreover, the Compact could include the use of the Universal Periodic Review to address recommendations to States, such as those regarding the protection of human rights of women and girls online. Clear focus should be on the strengthening of an open, free, secure and interoperable Internet that is a safe and trusted space for everyone through a multistakeholder model. Within this model the Freedom Online Coalition and the signatories of the Declaration for the Future of the Internet could be mentioned as relevant actors.

5 Accountability for discrimination and misleading content

5.1 Core principles

The Netherlands is committed to maintaining an open, free, secure, global, interoperable and reliable Internet. An Internet on which platforms regulate their content within the boundaries of democratic values, the rule of law, and in line with international human rights law. Despite all the social and economic benefits digitalization brings, it also entails risks and can be a facilitator of illegal content and activities, as well as harmful content.

Law enforcement, judicial oversight and cooperation with various stakeholders, including platforms and Internet Service Providers, therefore needs to be effective and legitimate. Key principles are: 1) respect for human rights, 2) lawfulness or legality, 3) proportionality, necessity and subsidiarity, 4) right to a fair trial and an effective right to remedy. For law enforcement to be successful, proportionate and trusted, cooperation with service providers is crucial, and whole-of-society prevention efforts for civilians and private entities are necessary. Only when citizens are safe to enjoy their rights and freedoms and when businesses can deploy commercial activities in a safe environment we can continue to reap the benefits of the digital age.

It is important that illegal content such as discriminatory or racist statements or child sexual abuse and exploitation material is removed from the Internet. Combating illegal content is both a task for Internet service providers, platforms as well as for the competent regulators. All of them will need to act adequately and transparently, with clear (appeal) procedures for users whose content has been removed.

For addressing harmful, but not illegal or unlawful (awful but lawful) content, the initiative lies mostly with the online platforms. Platforms can formulate and apply their terms of use in such a way that they can counter content that they find undesirable. This could also include misleading content and disinformation. But when applying this, these platforms will need to pay attention to international human rights law (including freedom of expression), including the UNGPBHR, and the legitimate interests of all stakeholders involved, including the users of the service.

5.2 Key commitments

The Netherlands is aware of calls for international standards in tackling harmful content online and emphasizes the importance of these being anchored in human rights obligations. Setting international standards for tackling harmful online content is especially challenging when it comes to unwanted, but not illegal, content. This is a complicated consideration where freedom of expression is the starting point and weighs particularly heavy, but where also tech platforms have significant freedom to determine for themselves what the terms of use of their services are.

The GDC should include commitments to strengthen the involvement of platforms and tech companies in shaping international standards around content moderation and governance. Civil society organizations and researchers are also conducting research into the (unintended) effects of such policies. Only with and through multistakeholder engagement can it be ensured that addressing harmful content is technically possible, feasible and enforceable and meets existing human rights obligations.

According to the Netherlands content moderation must be done on terms that are publicly known and understandable. Where platforms remove or otherwise moderate

unwanted, but not illegal content based on their terms of use, this must be done transparently and ensure that objections or appeals can be made. Furthermore, under the EU's Digital Services Act online platforms must clearly motivate their decisions to remove content. The GDC should therefore include commitments on transparency of content moderation criteria on platforms, which can be done in transparency reports. Transparency reports should provide clarity on the approach to both unlawful as well as harmful content.

Compliance with this obligation should be subject to independent supervision. The Netherlands is committed to compliance with the United Nations Guiding Principles on Business and Human Rights by tech companies.

6 **Promote regulation of artificial intelligence (AI)**

6.1 Core principles

It is important to recognise the potential of new and emerging technologies to bridge the digital divide between and within countries, and benefit people and the planet by driving inclusive growth, sustainable development and well-being. However, they can also amplify inequalities and stereotypes, and can cause harm, particularly to persons in vulnerable situations and marginalised groups. The Netherlands calls for a genderresponsive and human rights-based approach to the design, development, deployment, evaluation and use of technologies, platforms and tools (incl. AI and AIbased solutions) to ensure that (gender and racial) inequalities, stereotypes and biases are prevented and eradicated. Therefore, it is essential to promote international regulation of new and emerging technologies, focusing on a design that respects international law, including human rights law, the rule of law, democratic values, gender equality and diversity. Important safeguards, such as oversight and enforcement mechanisms should be in place to ensure accountability and liability.

6.2 Key commitments

In the field of AI, the European Union is a key partner in developing a human rightsbased approach. It has adopted and implemented several initiatives in this regard, such as the EU's AI Act and the Council of Europe's Convention on Artificial Intelligence (CAI). The Global Digital Compact provides an opportunity to bring this approach to the United Nations. The success of UNESCO's Recommendation on the Ethics of Artificial Intelligence indicates the importance of such an approach and gives us a foundation on which to build. By setting up an inclusive, multistakeholder process of international cooperation, the Global Digital Compact could create a framework for promoting the responsible use of AI while taking the interests of all stakeholders into account. The framework should address topics such as discrimination, privacy, transparency and explainability by and of AI. This could contribute positively to the overall goal of closing the digital divide and enabling equitable access to the benefits of AI while mitigating the risks.

7 Global Public Goods and Digital Commons

7.1 Core principles

Digital Public Goods (DPG) are crucial for inclusive, sustainable development and achieving the Sustainable Development Goals, particularly in the context of lowerand middle-income countries. The DPG Standard of the DPG Alliance² should be used as the standard to determine whether a digital solution conforms to the definition of a digital public good: open-source software, open data, open AI models, open standards, and open content that adhere to privacy and other applicable best practices, do no harm by design and are crucial for attainment of the United Nations 2030 Sustainable Development Goals. Digital commons are a separate category of goods that can also have great impact on realising the SDG's. The EU's experience with digital commons projects such as the European Digital Infrastructure Consortia as part of the Digital Decade policy program could benefit the discussion on a common set of principles and standards. The Netherlands has, together with other EU member states, shown interest in starting a European Digital Infrastructure Consortium to promote the development of digital commons within the EU.

7.2 Key commitments

The Global Digital Compact should strive for agreeing on principles and standards as underlined in the UN's road map: "Central to the implementation of digital public goods are robust human rights and governance frameworks to enhance trust in technology and data use, while ensuring inclusion". Moreover, the Compact should distinguish between digital commons and digital public goods, which both can play an important role for inclusive, sustainable development.

8 Other topics – linked to trusted connectivity

8.1 Core principles

8.1.1 Digital trust and security

One key prerequisite is a trustworthy and secure digital environment for all, including women, youth and people from marginalized communities, that will support the achievement of the SDGs by 2030. It should be stressed that human rights and cybersecurity are complementary, mutually reinforcing and interdependent. Our daily lives, economic prosperity, and social progress, depend on a trusted and secure digital environment that is affordable, accessible, and reliable. Oftentimes cyberspace is the backbone to equitable access to nearly all essential services, many provided by governments, including food, water, energy, healthcare, financial services as well as critical government functions, such as conducting elections. Security-by-design is therefore needed to embed cybersecurity in the core of the digital environment.

8.1.2 Sustainability

The Netherlands is committed to a sustainable digital transition, or twin transition. In light of the EU's Fit for 55 package, the Compact should reflect that our digital transition needs to be systemically aligned with the sustainability transformation to ensure that the digital infrastructure is itself comprehensively sustainable.

² https://digitalpublicgoods.net/who-we-are/#more

Furthermore, we need to develop and use digital innovations as an accelerating force for advancing our sustainable development agenda.

The aim of minimizing the environmental footprint of digital infrastructure, the internet and digital technologies could be achieved in various ways, for instance by promoting green data centres and supporting the deployment of sustainable telecoms infrastructure. Furthermore, the sustainability of software should not be forgotten and we also need to ensure that the digital transformation is supported by sufficient clean energy. Lastly, the importance of cross-border transfer of knowledge and experience should be emphasized, e.g. the fusion of innovative ecosystems.

8.2 Key commitments

8.2.1 Digital trust and security

The transnational and cross-cutting impacts of digital technologies require universal approaches that go beyond geographical borders and traditional siloes. Cyber capacity-building efforts are urgent and essential to safeguard and protect the digital environment as a foundation for sustainable development. We need to better understand the challenges faced by marginalized or disadvantaged groups and commit to supporting their paths towards improving internet access, manage digital risks and mitigate their impact. We will need an inclusive approach by states and other stakeholders, including private sector, civil society and academia, that takes into account existing initiatives, share best practices on building resilient digital networks and focus on practical capacity building efforts in this area.

8.2.2 Sustainability

In order to make these developments possible, unilateral government action is not sufficient. The Compact should therefore reflect the need for collaboration between governments and private actors in the digital sector, but also international collaboration between governments. Standardisation of sustainability factors, harmonization of policy instruments and better transparent reporting is important, but also the use of binding instruments should be seen as a viable option in ensure a clean digital transition.